EXHIBIT 12

Advocate Aurora Health Data Breach Affects 3 Million Patients

aapc.com/blog/86572-advocate-aurora-health-data-breach-affects-3-million-patients

By Lee Fifield October 27, 2022

Private health data was exposed through third-party tracking technology.

Advocate Aurora Health recently notified the U.S. Department of Health and Human Services Office for Civil Rights that it experienced a data breach on October 14. Advocate Aurora Health is a 26-hospital healthcare system in Wisconsin and Illinois with over 500 sites of care and $14 billion in annual revenue. The breach, which occurred through a tracking program from third-party vendors, may have compromised the private health information (PHI) of as many 3 million patients.

The Cause of the Breach

Following the breach, Advocate Aurora Health released a statement that disclosed how it uses third-party vendors to evaluate the trends and preferences of patients as they use the health system's websites. This tracking is accomplished through the use of pieces of code called pixels. The official statement explained, "We recently learned that, in certain circumstances, pixels or similar technologies installed on our patient portals available through MyChart and LiveWell websites and applications, as well as on some of our scheduling widgets, transmitted certain patient information to third-party analytics vendors that provided us with the pixel technology, particularly for users concurrently logged into their Facebook or Google accounts."

The breach especially affected those who were logged in to Facebook or Google when interacting on Advocate Aurora Health's websites or apps. The Meta Pixel tracking technology used (owned by Facebook's parent company Meta) sent patient PHI to Facebook as patients scheduled appointments and used the portal. Meta Pixel is a JavaScript tracker that follows user movement within a site in order to improve the patient experience and website operability.

Type of PHI Exposed

Patient information that may have been shared in the Advocate Aurora data breach includes:

- Dates, times, and/or locations of scheduled appointments
- IP address
- Proximity to an Advocate Aurora Health location
- Provider information
- Type of appointment or procedure scheduled
- Communications through the patient portal MyChart, which may have included patient name; medical record number; insurance status; and whether the patient had a proxy MyChart account, including the proxy's name

Advocate Aurora Health's investigation into the incident showed that no social security numbers, payment methods, or financial information were involved in the breach.

Steps Taken

Out of an abundance of caution, Advocate Aurora Health decided to assume that all patients were affected and informed every patient about the breach. The health system has disabled and/or removed pixels and related technology from its platforms. An internal investigation is currently underway to better understand what patient information was transmitted to third-party vendors. According to officials, it is not yet clear whether browser type, browser configuration, cookies, personal Facebook or Google accounts, or the specific actions of users played a role in the release of their data.

Legal Action

The Advocate Aurora Health data breach was not the first of its kind. A similar breach was reported by Novant Health in August that affected more than 1 million patients, and there may be other breaches of which hospitals are unaware. A June report from The Markup, a

non-profit newsroom that investigates how institutions are using technology to change society, found the Meta Pixel tracker used in 33 of the top 100 hospitals in America.

Patients of Advocate Aurora Health have filed a class action complaint against the health system, seeking financial relief to the tune of more than $5 million in damages, and complaints and lawsuits continue to be filed against numerous hospitals for HIPAA violations associated with Meta Pixel and Facebook parent company Meta for illegal data mining practices and use of PHI for profit, though it should be noted that Meta is not bound by HIPAA rules; it is more likely the hospitals that use the tracking technology would be found in violation of HIPAA for transferring patient data without consent. A plaintiff in a separate lawsuit alleges that they have identified at least 664 hospital systems from which Facebook has received PHI via Meta Pixel.

One attorney noted that patients may falsely assume that because their medical providers protect their health information under HIPAA that it's not being disclosed, but that is not the case. "If you walk into [a medical] office, you have to sign a HIPAA form. With Pixel, there's no such thing," said Carol Villegas, a partner at Labaton Sucharow LLP.

Resources:

https://www.healthcaredive.com/news/advocate-aurora-health-breach-3-million-patient-information/634662/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-10-21%20Healthcare%20Dive%20%5Bissue:45448%5D&utm_term=Healthcare%20Dive

https://www.advocateaurorahealth.org/pixel-notification/faq

https://www.advocateaurorahealth.org/pixel-notification/

https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

Comments are closed.